ABSTRACT OF THE DISCLOSURE

Methods and apparatus for providing a centralized source of session keys to be shared by a Home Agent and a Mobile Node are disclosed. In accordance with one aspect of the invention, a Mobile Node registers with a Home Agent supporting Mobile IP by sending a registration request to the Home Agent. The Home Agent sends a request message (e.g., access-request message) to a AAA server, the request message identifying the Mobile Node. The AAA server then derives key information from a key or password associated with the Mobile Node. The AAA server then sends a reply message (e.g., access-reply message) to the Home Agent, the reply message including the key information associated with the Mobile Node, thereby enabling the Home Agent to derive a shared key to be shared between the Mobile Node and the Home Agent from the key information. The Home Agent derives a key from the key information, the key being a shared key between the Mobile Node and the Home Agent. A registration reply is then sent to the Mobile Node. When the Mobile Node receives a registration reply from the Home Agent, the registration reply indicates that the Mobile Node is to derive a key to be shared between the Mobile Node and the Home Agent. The Mobile Node then derives a key to be shared between the Mobile Node and the Home Agent from key information stored at the Mobile Node. The Mobile Node may initiate "re-keying" by sending a subsequent registration request to the Home Agent.